IN THE CLAIMS:

1. canceled

2. canceled

3. canceled

4. canceled

5. (currently amended) A system for producing multiple-symbol non-repeating randomizer sequences over GF(2^m), the system including:

A. a first register for supplying an initial state, the register holding a non-zero element of GF(2^m);

B. a first multiplier for multiplying the contents of the register by a multiplier constant that is a primitive element of GF(2^m); and

C. first feedback means for

i. supplying the products produced by the multiplier as the symbols of the randomizer sequence,

ii. supplying the symbols of the randomizer sequence to update the first register, and

~~The system of claim 1 further including~~ D. encryption means for encrypting a code word, the encryption means including:

~~a.~~i. selection means for selecting an initial state for use in producing the randomizer sequence;

~~b.~~ii.means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over GF(2^m), the means producing a randomized code word; and

~~c.~~iii. means for producing a key associated with the selected the initial state.

6. (original) The system of claim 5 further including a decrypting subsystem for using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

7. (currently amended) ~~The system of claim 1 wherein the multiplier constant~~ A system for producing multiple-symbol non-repeating randomizer sequences over GF(2^m), the system including:

A. a first register for supplying an initial state, the register holding a non-zero element of GF(2^m);

B. a first multiplier for multiplying the contents of the register by a multiplier constant that is a primitive element of GF(2^m) which is selected to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code; and

C. first feedback means for

i. supplying the products produced by the multiplier as the symbols of the randomizer sequence, and

ii. supplying the symbols of the randomizer sequence to update the first register.

8. (original) The system of claim 6 further including means for detecting mis-synchronization, the mis-synchronization detection means including:

a. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over GF(2^m), the means producing a randomized code word;

b. means for removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. a decoder for decoding the reproduced ECC code word, the decoder detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

9. canceled

10. canceled

11. canceled

12. (currently amended) A system for producing multiple-symbol non-repeating randomizer sequences over GF(2^m), the system including:

A. a first register for supplying an initial state, the register holding a non-zero element of GF(2^m);

B. a first multiplier for multiplying the contents of the register by a multiplier constant that is a primitive element of GF(2^m); and

C. first feedback means for

i. supplying the products produced by the multiplier as the symbols of the randomizer sequence, and

ii. supplying the symbols of the randomizer sequence to update the first register.

D. one or more second registers for holding elements of GF(2^m);

E. one or more second multipliers for multiplying the contents of the one or more second registers by one or more multiplier constants that are elements of GF(2^m);

F. an adder for adding the products produced by the first and second multipliers and supplying the sum to the first feedback means;

G. second feedback means for supplying the contents of the first register to update the second register; and

~~The system of claim 11 further including~~

H. means for detecting mis-synchronization, the mis-synchronization detection means including:

a. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word;

b. means for removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. a decoder for decoding the reproduced ECC code word, the decoder detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

13. (original) The system of claim 12 wherein the multiplier constants are further selected from a set of multiplier constants that produce randomizer sequences that are at least a predetermined minimum distance from code words of a given BCH code.

14. (original) The system of claim 13 further including a means for providing a key to select the multiplier constants for a given the randomizer sequence.

15. canceled

16. canceled.

17. (currently amended) A system for producing multiple-symbol non-repeating randomizer sequences over $GF(2^m)$, the system including:

A. a first register for supplying an initial state, the register holding a non-zero element of $GF(2^m)$;

B. a first multiplier for multiplying the contents of the register by a multiplier constant that is a primitive element of $GF(2^m)$; and

C. first feedback means for

i. supplying the products produced by the multiplier as the symbols of the randomizer sequence, and

ii. supplying the symbols of the randomizer sequence to update the first register

D. a plurality of second multipliers each for multiplying the contents of the register by a multiplier constant that is a primitive element of $GF(2^m)$;

E. a switch for selecting one of the plurality of second multipliers or the first multiplier to produce the randomizer sequence; and

F. ~~The system of claim 16 further including~~ encryption means for encrypting a code word, the encryption means including:

i~~d~~. selection means for selecting an initial state for use in producing the randomizer sequence;

ii~~e~~. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$, the means producing a randomized code word; and

~~f.~~iii. means for producing a key associated with the selected the initial state.

18. (original) The system of claim 17 further including decryption means for using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

19. (original) The system of claim 18 wherein the selection means further selects the multiplier constant from a set of multiplier constants.

20. (currently amended) A system for producing multiple-symbol non-repeating randomizer sequences over $GF(2^m)$, the system including:

A. a first register for supplying an initial state, the register holding a non-zero element of $GF(2^m)$;

B. a first multiplier for multiplying the contents of the register by a multiplier constant that is a primitive element of GF(2^m); and

C. first feedback means for

i. supplying the products produced by the multiplier as the symbols of the randomizer sequence, and

ii. supplying the symbols of the randomizer sequence to update the first register;

D. one or more second registers for holding elements of GF(2^m);

E. one or more second multipliers for multiplying the contents of the first register by associated elements of GF(2^m) and supplying the products to update the one or more second registers;

F. one or more adders for adding the contents of the one or more second registers to the product produced by the first multiplier to produce a sum and supplying the sum to the first feedback means; and

G. ~~The system of claim 15 further including~~ encryption means for encrypting a code word, the encryption means including:

~~g.~~i. selection means for selecting an initial state for use in producing the randomizer sequence;

~~h.~~ii. means for combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over GF(2^m), the means producing a randomized code word; and

~~i.~~iii. means for producing a key associated with the selected the initial state.

21. canceled

22. canceled

23. canceled

24. canceled

25. canceled

26. canceled

27. canceled

28. canceled

29. (currently amended) A method for producing multiple-symbol non-repeating randomizer sequences over GF(2^m), the method including the steps of:

A. supplying an initial state to a first register;

B. selecting a multiplier constant to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code and producing a first product by multiplying the contents of the first register by the multiplier constant that is a primitive element of GF(2^m);

C. supplying the first product as

a. a next symbol of the randomizer sequence, and

b. an update to the first register;

D. repeating steps A-C i times for $i \leq 2^m-2$; and

~~The method of claim 28 further including the step of~~

E. detecting mis-synchronization by

a. combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over GF(2^m), to produce a randomized code word;

b. removing the randomizer sequence from the randomized code word to reproduce the ECC code word; and

c. decoding the reproduced ECC code word and detecting a mis-synchronization if the number of errors in the reproduced ECC code word is greater than the number of errors that can be corrected by the given BCH code.

30. canceled

31. (currently amended) A method for producing multiple-symbol non-repeating randomizer sequences over $GF(2^m)$, the method including the steps of:

A. supplying an initial state to a first register;

B. selecting a multiplier constant to produce randomizer sequences that are each a predetermined minimum distance from code words of a given BCH code and producing a first product by multiplying the contents of the first register by the multiplier constant that is a primitive element of $GF(2^m)$;

C. supplying the first product as

a. a next symbol of the randomizer sequence, and

b. an update to the first register;

D. repeating steps A-C i times for $i \leq 2^m-2$; and

~~The method of claim 30 further including the step of~~

E. providing a key to select the multiplier constants associated with a given randomizer sequence.

32. canceled

33. canceled

34. (currently amended) A method for producing multiple-symbol non-repeating randomizer sequences over $GF(2^m)$, the method including the steps of:

A. supplying an initial state to a first register;

B. producing a first product by multiplying the contents of the first register by a multiplier constant that is a primitive element of $GF(2^m)$;

C. supplying the first product as

a. a next symbol of the randomizer sequence, and

b. an update to the first register;

D. repeating steps A-C i times for $i \leq 2^m-2$; and

~~The method of claim 23 further including a step of~~

E. encrypting a code word by:

~~j.~~a. selecting an initial state for use in producing the randomizer sequence;

~~k.~~b. combining the randomizer sequence with an ECC code word that is encoded in accordance with a given BCH code over $GF(2^m)$ to produce a randomized code word; and

~~l.~~c. producing a key associated with the selected the initial state.

35. (original) The method of claim 34 further including a step of decrypting the code word by using the key to reproduce the randomizer sequence and removing the randomizer sequence from the randomized code word to reproduce the ECC code word.

36. (original) The method of claim 34 wherein the step of selecting the initial state further includes selecting one or more multiplier constants.